VICTOR JIH, SBN 186515
vjih@wsgr.com
KELLY H. YIN, SBN 328380
kyin@wsgr.com
WILSON SONSINI GOODRICH & ROSATI, P.C.
1900 Avenue of The Stars,
28th Floor
Los Angeles, CA 90067
Telephone: (424) 446-6900
Facsimile: (866) 974-7329

LUIS LI, SBN 156081
luis.li@wsgr.com
WILSON SONSINI GOODRICH & ROSATI, P.C.
953 East Third Street
Suite 100
Los Angeles, CA 90013
Telephone: (323) 210-2900

SHERYL S. BASSIN, NY SBN 4662797
sbassin@wsgr.com
(admitted *pro hac vice*)
DYLAN G. SAVAGE, CA SBN 310452
dsavage@wsgr.com
WILSON SONSINI GOODRICH & ROSATI, P.C.
1301 Avenue of the Americas.
40th Floor
New York, NY 10019
Telephone: (212) 999-5800
Facsimile: (866) 974-7329

THOMAS WAKEFIELD, SBN 330121
twakefield@wsgr.com
WILSON SONSINI GOODRICH & ROSATI, P.C.
One Market Plaza, Spear Tower,
Suite 3300
San Francisco, CA 94105
Telephone: (424) 446-6900

Attorneys for Defendants TikTok Inc. and ByteDance Inc.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

BERNADINE GRIFFITH, et al., Individually and on behalf of all others similarly situated,

Plaintiffs,

v.

TIKTOK INC., a corporation; BYTEDANCE, INC. a corporation,

Defendants.

Case No. 5:23-cv-0964-SB-E

JOINT BRIEF RE DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

Judge: Hon. Stanley Blumenfeld, Jr.
Date: 11/1/2024
Time: 8:30 a.m.
Place: Courtroom 6C

Action Filed: May 26, 2023
Trial Date: January 20, 2025

TABLE OF CONTENTS

Page

I. INTRODUCTORY STATEMENTS 1

A. Defendants' Introduction 1

B. Plaintiffs' Introduction 2

II. LEGAL STANDARD 3

A. DEFENDANTS' STATEMENT 3

B. PLAINTIFFS' STATEMENT 3

III. ISSUE NO. 1: PRIVATE INFORMATION 4

A. DEFENDANTS' POSITION: There is no evidence that any private information about Plaintiffs was disclosed to Defendants 4

1. Plaintiffs have not shown that the Pixel transmitted their sensitive, identifying information 5

2. Plaintiffs have not shown that EAPI transmitted their identifying or sensitive information 9

B. PLAINTIFFS' POSITION: Defendants' Sample Data Provides Evidence of Their Collection of Identifying Private Information from Plaintiffs 10

1. Defendants Misstate Applicable Law 10

2. Sample Data from Defendants' Own Servers Provides Sufficient Evidence to Defeat Summary Judgment 11

3. Defendants' Caselaw Is Unavailing. 18

IV. ISSUE NO. 2: INTERCEPTION 19

A. DEFENDANTS' POSITION: There is no evidence that Defendants intercepted the contents of Plaintiff's communications 19

1. The Pixel did not intercept the contents of Plaintiffs' communications 19

2. EAPI did not intercept the contents of Plaintiffs' communications 21

B. PLAINTIFFS' POSITION: Factual Disputes on "Contents" and "Interception" Preclude Summary Judgment. 21

1. "Contents" 21

2. "Interception" 23

V. ISSUE NO. 3: CONSENT 25
A. DEFENDANTS' POSITION: Plaintiffs consented to advertisers' use of the Pixel and EAPI. 25
1. Plaintiffs expressly consented when they created accounts 25
a) Rite Aid 26
b) Hulu 27
c) Etsy 29
d) Upwork 30
2. Plaintiffs impliedly consented by conduct 32
B. PLAINTIFFS' POSITION: A Reasonable Juror Could Find There Was No Consent. 33
1. No Express Consent 34
a) No Privacy Policy Mentions Defendants 34
b) The Privacy Policy Disclosures About Data Collection Are Generalized and Ambiguous 35
i. Rite Aid 35
ii. Hulu 36
iii. Etsy 37
iv. Upwork 38
v. Other Websites 39
2. No Implied Consent 39
VI. ISSUE NO. 4: PROPERTY 41
A. DEFENDANTS' POSITION: There is no evidence that Defendants took Plaintiffs' property 41
B. PLAINTIFFS' POSITION: Plaintiffs Have a Recognized Property Interest In Their Data, Which Has Monetary Value 43
VII. CONCLUSION 44
A. Defendants' Conclusion 44
B. Plaintiffs' Conclusion 44

TABLE OF AUTHORITIES

Page(s)

CASES

A.B. v. Google, Inc.,
2024 WL 3052969 (N.D. Cal. Jun. 18, 2024) 43

A.S. v. SelectQuote Ins. Servs.,
2024 WL 3881850 (S.D. Cal. Aug. 19, 2024) 5

Anderson v. Liberty Lobby, Inc.,
477 U.S. 242 (1986) 3

Berry v. Funk,
146 F.3d 1003 (D.C. Cir. 1998) 32, 41

Brodsky v. Apple Inc.,
445 F. Supp. 3d 110 (N.D. Cal. 2020) 19

Brown v. Google,
685 F.Supp.3d 909 (N.D. Cal. 2023) 10, 11, 16, 22, 34

Byars v. Sterling Jewelers, Inc.,
2023 WL 2996686 (C.D. Cal. Apr. 5, 2023) (Blumenfeld, J.) 4, 10, 18

Calhoun v. Google, LLC,
113 F.4th 1141 (9th Cir. 2024) 33, 34, 35, 43

Calhoun v. Google LLC,
526 F.Supp.3d 605 (N.D. Cal. 2021) 25, 43, 44

Celotex Corp. v. Catrett,
477 U.S. 317 (1986) 3

Comprehensive Med. Ctr., Inc. v. State Farm Mut. Auto. Ins.,
690 F. Supp. 3d 1104 (C.D. Cal. 2023) 5, 17

CTC Real Estate Services v. Lepe,
140 Cal.App.4th 856 (Cal. App. 2006) 44

Digital Envoy, Inc. v. Google, Inc.,
370 F.Supp.2d 1025 (N.D. Cal. 2005) 34

Doe I v. Google LLC,
2024 WL 3490744 (N.D. Cal. July 22, 2024) 41, 43

Drenckhahn v. Costco Wholesale Corp.,
2010 WL 11508344 (C.D. Cal. Jun. 3, 2010) 4

Flanagan v. Flanagan,
41 P.3d 575 (Cal. 2002) 19, 21, 24

Flannery v. American Express Corp.,
2024 WL 648689 (C.D. Cal., Jan 29, 2024) 43

Griffith v. TikTok, Inc.,
697 F. Supp. 3d 963 (N.D. Cal. 2023) 33, 43

Griggs-Ryan v. Smith,
904 F.2d 112 (1st Cir. 1990) 32, 40

Gruber v. Yelp, Inc.,
55 Cal.App.5th 591 (Cal. App. 2020) 23

Hammerling v. Google LLC,
615 F. Supp. 3d 1069 (N.D. Cal. 2022),
aff'd, 2024 WL 937247 (9th Cir. Mar. 5, 2024) 4, 16, 18, 20, 21

Hill v. Nat'l Collegiate Athletic Ass'n.,
865 P.2d 633 (Cal. 1994) 32, 41

In re Facebook, Inc. Internet Tracking Litig.,
956 F.3d 589 (9th Cir. 2020) 44

In re Google Referrer Header Priv. Litig.,
465 F.Supp.3d 999 (N.D. Cal. 2020) 10

In re Google RTB,
606 F.Supp.3d 935 (N.D. Cal. 2022) 19, 22

In re Google RTB Consumer Priv. Litig.,
2024 WL 2242690 (N.D. Cal. Apr. 4, 2024) 10, 17

In re Meta Pixel Healthcare Litig.,
647 F. Supp. 3d 778 (N.D. Cal. 2022) 4, 22, 34

In re Meta Pixel Tax Filing Cases,
2024 WL 1251350 (N.D. Cal. Mar. 24, 2024) 43

In re Nickelodeon Consumer Priv. Litig.,
827 F.3d 262 (3d Cir. 2016) 5, 18, 19

In re Oracle Corp. Secs. Litig.,
627 F.3d 376 (9th Cir. 2010) 3

In re Yahoo Mail Litig.,
308 F.R.D. 577 (N.D. Cal. 2015) 40

In re Yahoo Mail Litig.,
7 F. Supp. 3d 1016 (N.D. Cal. 2014) 26

Javier v. Assurance IQ, LLC,
2022 WL 1744107 (9th Cir. May 31, 2022) 40

Keebaugh v. Warner Bros. Ent. Inc.,
100 F.4th 1005 (9th Cir. 2024) 26

Kis v. Cognism, Inc.,
2024 WL 3924553 (N.D. Cal. Aug. 23, 2024) 43

Konop v. Hawaiian Airlines, Inc.,
302 F.3d 868 (9th Cir. 2002) 19, 21, 24

Kremen v. Cohen,
337 F.3d 1024 (9th Cir. 2003) 42

Lau v. Gen Digit. Inc.,
2024 WL 1880161 (N.D. Cal. Apr. 3, 2024) 42

Lindsey v. City of Pasadena,
2018 WL 11249917 (C.D. Cal. Feb. 5, 2018) 3

Low v. LinkedIn Corp.,
900 F. Supp. 2d 1010 (N.D. Cal. 2012) 42, 43

M.R. v. Salem Health Hospitals and Clinics,
2024 WL 3970796 (D. Or. Aug 28, 2024) 43

Masson v. New Yorker Mag., Inc.,
501 U.S. 496 (1991) 3

Matsushita Elec. Indus. Co. v. Zenith Radio,
475 U.S. 574 (1986) 3

Med. Lab'y Mgmt. Consultants v. Am. Broad. Co.,
306 F.3d 806 (9th Cir. 2002) 6

Opperman v. Path,
205 F.Supp.3d 1064 (N.D. Cal. 2016) 34

Rodriguez v, Google LLC,
2024 WL 38302 (N.D. Cal. Jan. 3. 2024) 39, 40

Rojas v. HSBC Card Servs. Inc.,
93 Cal. App. 5th 860 (2023) 32

Smith v. Facebook, Inc.,
262 F. Supp. 3d 943 (N.D. Cal. 2017),
aff'd, 745 F. App'x 8 (9th Cir. 2018) 26

Smith v. Facebook, Inc.
745 F.App'x 8 (9th Cir. 2018) 33

Smith v. Maryland,
442 U.S. 735 (1979) 42

Tanner v. Acushnet Co.,
2023 WL 8152104 (C.D. Cal. Nov. 20, 2023) 42

United States v. Alexander,
106 F.3d 874 (9th Cir. 1997) 33

United States v. Forrester,
512 F.3d 500 (9th Cir. 2008) 22

United States v. Szymuszkiewicz,
622 F.3d 701 (7th Cir. 2010), *as amended* (Nov. 29, 2010) 24

Valenzuela v. Kroger Co.,
2023 WL 4418887 (C.D. Cal. June 23, 2023) 21, 24

Van Patten v. Vertical Fitness Grp., LLC,
847 F.3d 1037 (9th Cir. 2017) 33

Wall v. Wescom Central Credit Union,
2024 WL 1158361 (C.D. Cal. Mar 18, 2024) 43

Wesch v. Yodlee, Inc.,
2021 WL 1399291 (N.D. Cal. Feb. 16, 2021) 10

STATUTES

Cal. Penal Code § 631 19

Cal. Penal Code § 632 ..... 4, 19, 25, 33

Children's Online Privacy Protection Act 18

Electronic Communications Privacy Act 10, 19, 21, 22, 23, 24, 32

RULES

Fed. R. Civ. P. 56(a) 3

Fed. R. Civ. P. 37(e)(1) 2, 12

TABLE OF ABBREVIATIONS

SAC	Second Amended Class Action Complaint, ECF No. 137
Defendants	TikTok Inc. and ByteDance Inc.
EAPI	Events Application Programming Interface ("API")
Ex. __	Exhibit(s) attached to the Joint Appendix of Evidence, filed contemporaneously herewith
Plaintiffs	Bernadine Griffith, Jacob Leady (Watters), and Patricia Shih
TikTok	The TikTok platform
TTI	TikTok Inc.

I. INTRODUCTORY STATEMENTS

A. Defendants' Introduction

Plaintiffs have long claimed that TikTok surreptitiously collected their sensitive, personally-identifying information, but they cannot show those allegations are true—indeed, the evidence is to the contrary. Defendants provide advertisers with commonplace software tools, the Pixel and Events API ("EAPI"), that can be installed on a website (Pixel) or server (EAPI) to collect information about internet activity to improve their advertising on TikTok. Ex. 3 at 38:5-10, 48:8-10; JAF-1; JAF-2. The advertisers and website owners control whether to use the tools, how to configure them, and how to provide notice to their customers. Ex. 3 at 38:5-10, 38:17-22 39:6-10, 48:14-17, 141:10-13; JAF-3; JAF-4. Plaintiffs claim that six advertisers—Rite Aid, Hulu, Etsy, Upwork, Build-A-Bear, and Sweetwater—used the tools to invade Plaintiffs' privacy, gather Plaintiffs' sensitive information, and share that information with Defendants. But the evidence does not bear this theory out. Instead, it shows ordinary internet data practices that do not invade privacy or property interests.

At this stage, Plaintiffs can no longer rely on allegation, speculation, and generalization about a putative class. They now must show, *with evidence*, that *their* privacy was *actually* invaded. As the Court recognized in recent rulings, Plaintiffs have not made that showing. They *cannot* make it because the facts do not bear out the premises of their case: there is no evidence that their sensitive, individually-identifying information was disclosed to Defendants; there is no evidence that their communications were intercepted "in transit"; there *is* evidence that Plaintiffs expressly and impliedly consented to data collection and transmission; and there is no evidence that they had a property interest in any data that was transmitted. On these independent grounds, summary judgment should be granted on all counts.[1]

[1] Per Plaintiffs, Cantore will be dismissing his claims with prejudice.

B. Plaintiffs' Introduction

This case is not about six websites. It is about Defendants' taking Plaintiffs' data from tens of thousands of websites for years. Notwithstanding Defendants' spoliation of the most direct evidence of their collection of Plaintiffs' data, which is the subject of a separate Rule 37(e)(1) motion, Plaintiffs have still adduced sufficient evidence that precludes summary judgment on all issues raised by Defendants.

First, the evidence shows that Defendants collected Plaintiffs' information. This evidence comes in at least two forms: (1) samples of the data that Defendants collected on non-TikTok users on March 28, 2024 and May 21, 2024 ("two-day sample"); and (2) Plaintiffs' own browsing histories on websites that use the Pixel or EAPI. The collected data includes [redacted] although this is not a requirement to establish liability, and [redacted] And the jury may extrapolate from the two-day sample to understand the scope of Defendants' collection.

Second, Plaintiffs have established that the Pixel [redacted] and that [redacted]" It is further undisputed that Defendants [redacted]. Thus, there are triable factual issues on whether Pixel and EAPI contemporaneously intercept contents of communications.

Third, Defendants have not established either express or implied consent. No privacy policy cited by Defendants even mentions them specifically, let alone the extent of data that they collect on non-TikTok users through non-TikTok websites. That Plaintiffs continued to browse the internet after joining this action does not establish implied consent—especially as to the time period before joining.

Fourth, Plaintiffs have a property interest in their personal data. Not only does the weight of legal authority hold as much, but Plaintiffs' damages expert has

calculated actual monetary damages based on his analysis of similar market measures. Defendants' motion should be denied in its entirety.

II. LEGAL STANDARD

A. DEFENDANTS' STATEMENT

Summary judgment is appropriate where the record, read in the light most favorable to the non-moving party, shows that "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *see also Celotex Corp. v. Catrett*, 477 U.S. 317, 322-23 (1986). Material facts are those necessary to prove or defend a claim, as determined by reference to substantive law. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986).

The moving party bears the initial burden of establishing the absence of a genuine issue of material fact and can satisfy this burden by showing "that there is an absence of evidence to support the nonmoving party's case." *Celotex*, 477 U.S. at 325. If this initial burden is met, "the burden then shifts to the non-moving party to designate specific facts demonstrating the existence of genuine issues for trial." *In re Oracle Corp. Secs. Litig.*, 627 F.3d 376, 387 (9th Cir. 2010). "If the evidence is merely colorable, or is not significantly probative," there is no genuine dispute and "summary judgment may be granted." *Liberty Lobby*, 477 U.S. at 249-50.

B. PLAINTIFFS' STATEMENT

"On summary judgment, [the court] must draw all justifiable inferences in favor of the nonmoving party, including questions of credibility and of the weight to be accorded particular evidence." *Masson v. New Yorker Mag., Inc.*, 501 U.S. 496, 520 (1991). Summary judgment may be granted only if "the record taken as a whole could not lead a rational trier of fact to find for the non-moving party." *Matsushita Elec. Indus. Co. v. Zenith Radio*, 475 U.S. 574, 587 (1986).

"In order to survive summary judgment, a Plaintiff need not prove their case to the Court's satisfaction, rather they need only raise a genuine issue of material fact such that a reasonable jury could find in favor of Plaintiffs." *Lindsey v. City of*

Pasadena, 2018 WL 11249917, at *6 (C.D. Cal. Feb. 5, 2018); *Drenckhahn v. Costco Wholesale Corp.*, 2010 WL 11508344, at *5 (C.D. Cal. Jun. 3, 2010) ("Plaintiff need not prove his case; he need only identify enough evidence such that a reasonable jury might return a verdict in his favor.").

III. ISSUE NO. 1: PRIVATE INFORMATION

A. DEFENDANTS' POSITION: There is no evidence that any private information about Plaintiffs was disclosed to Defendants

Defendants are entitled to summary judgment on Plaintiffs' privacy and wiretapping claims (Counts 1, 4, and 5) because there is no evidence that advertisers' use of the Pixel or EAPI disclosed Plaintiffs' sensitive, identifying information to Defendants.

To state any privacy or CIPA § 632(a) claim, Plaintiffs must establish, inter alia, "(1) a legally protected privacy interest, (2) a reasonable expectation for privacy, and (3) the intrusion is so serious as to amount to an egregious breach of the social norms." *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1088 (N.D. Cal. 2022), *aff'd*, 2024 WL 937247 (9th Cir. Mar. 5, 2024); *see also In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 798, 800 & n.12 (N.D. Cal. 2022) (applying that framework to CIPA § 632(a)). Data "implicates a protectable privacy interest" subject to a reasonable expectation of privacy when it is "sensitive" and related to "specific personal information." *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5, 2023) (Blumenfeld, J.).

Thus, Plaintiffs must present evidence that Defendants collected information that is both sensitive and identifying, thereby invading Plaintiffs' reasonable expectation of privacy in a manner highly offensive to a reasonable person. *See Hammerling*, 615 F. Supp. 3d at 1089. Plaintiffs cannot carry that burden. *See* ECF No. 242 (Class Cert. Order) at 15, 16 n.10; ECF No. 248 (Order) at 2.

1. Plaintiffs have not shown that the Pixel transmitted their sensitive, identifying information

Browsing the internet necessarily involves sharing basic information. Gathering that information, without more, is not actionable—and ultimately, Plaintiffs cannot even show such commonplace gathering of their information by Defendants, let alone an invasion of privacy.

Plaintiffs assert that they browse the internet—including the Rite Aid, Hulu, Etsy, Upwork, Build-A-Bear, and Sweetwater websites,[2] which use the Pixel. *See* ECF No. 137 (SAC) ¶¶ 107-24, 130-35.[3] Plaintiffs complain that these advertisers collect browsing information such as a timestamp, IP address, User Agent, cookies, and certain URLs. *See, e.g.*, Ex. 30 ¶¶ 58-63. But the collection of such information is how the internet works—not something unique to the Pixel, Ex. 28 ¶ 33; *see* JAF-9—and is not actionable. *See In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 283 (3d Cir. 2016) ("static digital identifiers that could, in theory, be combined with other information to identify a person do not count as 'personally identifiable information'"). And there is "no evidence that Defendants can identify who the person is that generated the data absent the collection of personally identifying information (PII) such as name, address, phone number, or email address linked to the IP address and user agent." ECF No. 242 (Class Cert. Order) at 4; *see also A.S. v. SelectQuote Ins. Servs.*, 2024 WL 3881850, at *1 (S.D. Cal. Aug. 19, 2024).

---

[2] Sweetwater is "not mentioned in the SAC," ECF No. 242 (Class Cert. Order) at 3, and a movant's burden at summary judgment is "is framed by the allegations in the pleadings." *Comprehensive Med. Ctr., Inc. v. State Farm Mut. Auto. Ins.*, 690 F. Supp. 3d 1104, 1114 (C.D. Cal. 2023). Thus, any Sweetwater-related evidence cannot help Plaintiffs. But, as explained below, that evidence no more supports Plaintiffs claims than does the evidence regarding other advertisers.

[3] Plaintiffs allege The Vitamin Shoppe and Feeding America also "installed the TikTok Pixel." ECF No. 242 (Class Cert. Order) at 3. [redacted]

To establish a privacy violation, Plaintiffs must show that these advertisers sent Defendants something *more*—something sensitive and identifying. Plaintiffs attempt to do so by claiming that sensitive, identifying information *could* be transferred to Defendants through full-string URLs. *See* ECF No. 242 at 16. But that theory runs aground on the evidence.

As the Court recently ruled, it is not enough to assert that "a URL *can* contain sensitive information"; Plaintiffs must "show[] that the URLs sent to Defendants based on their own browsing history *did*." ECF No. 242 at 16. But Plaintiffs do not even allege, let alone "provide evidence that any named plaintiff searched for … sensitive items … on any other site that uses the Pixel." *Id.* at 16 n.10. Plaintiffs cannot show that their sensitive, identifying information was captured on these websites, [redacted] Ex. 29 ¶¶ 17-19, 80-87.

In addition to lacking evidence on the front end that the advertisers' sites were gathering their sensitive, identifying data through the Pixel, Plaintiffs' theory also fails on the back end: "Plaintiffs lack evidence of any information collected by Defendants from the named plaintiffs." ECF No. 248 at 2. "[B]ecause the named Plaintiffs have not produced evidence of any data collected from them, it is not even clear that they have suffered any cognizable injury." ECF No. 242 at 15. And it would not be enough to simply show that "any data" was collected—Plaintiffs would need to show that Defendants received *sensitive* information, personally identifiable to them. *See id.* at 10 ("[T]he information collected from non-TikTok users cannot uniformly be linked to their identities because TikTok does not have user profiles for them."); *Med. Lab'y Mgmt. Consultants v. Am. Broad. Co.*, 306 F.3d 806, 814 (9th Cir. 2002) (affirming summary judgment when plaintiff lacked evidence that personal, sensitive information was disclosed).

Plaintiffs cannot make that showing because, far from supporting Plaintiffs' claims, the evidence undercuts their theory that advertisers collected sensitive, identifying information about Plaintiffs and disclosed it to Defendants:

Griffith. There is no browsing-history evidence that Griffith ran searches on the Rite Aid, Hulu, Etsy, or Build-A-Bear websites, much less searches that revealed sensitive and identifying information. *See* Exs. 11-12; JAF-15.[4] There is also no evidence that Griffith visited a URL on the Rite Aid, Hulu, Etsy, or Build-A-Bear websites that could reveal sensitive or identifying information. Exs. 11-12; *see* JAF-10. The evidence shows that Griffith neither created a Build-A-Bear account nor purchased Build-A-Bear products online. *See* Ex. 8; *see also* JAF-12. Build-A-Bear could not even determine whether Griffith had ever visited the site. *Id.* And even if Griffith could identify some sensitive Hulu information, [redacted] *See* Ex. 13 at 1; Ex. 2 at 173:25-176:21; JAF-12. [redacted]. *See* Ex. 14 at 1; Ex. 15 at 1; Ex. 16 at 1; JAF-12.

Shih. Shih's browsing history shows no TTI cookies associated with the subject websites. *See* Ex. 28 ¶¶ 81-82; JAF-19. There is no browsing-history evidence that Shih ran searches on Etsy, Hulu, or Upwork websites, much less searches that revealed sensitive, identifying information. Exs. 21-24; JAF-16. There is also no evidence that Shih visited a URL associated with the Etsy, Hulu, or Upwork websites that revealed sensitive or identifying information. *Id.*[5] Shih has not had an active Hulu account since 2013 and never even logged into her Hulu profile, except to produce discovery in this litigation. *See* Ex. 5 at 205:13-206:14,

---

[4] [redacted] *See* Ex. 2 at 220:8-222:1; JAF-15. Assuming these searches happened, the Pixel could not have included an email address or phone number (hashed or unhashed) because she did not provide that information as part of her search.

[5] [redacted] Ex. 22 at Browser History tab, row 16. Because Shih was not logged-in, the Pixel could not have captured any identifying data about her. *See* Ex. 5 at 220:18-22; JAF-13.

212:2-9; JAF-13. Indeed, Shih never used Hulu on her browser except for visits for purposes of this litigation and a single visit long after she discontinued her account. *See* Ex. 5 at 216:12-217:25, 266:21-271:18; JAF-13. Defendants did not receive any identifying data from that visit. *See* Ex. 29 ¶¶ 30-38, 84-85. There is no evidence the Pixel obtained any browsing information from Etsy, Hulu, or Upwork—let alone sensitive information. Ex. 28 ¶¶ 81-82; JAF-20. Not only has Shih failed to identify any sensitive information, but also there is no evidence that such information would be identifying. To the contrary, Shih testified that she uses Apple's Hide My IP Address feature on Safari. *See* Ex. 5 at 135:9-13, 183:15-21; JAF-20. She also typically uses uBlock Origin and Ghostery when she browses the internet to block ads and cookies and to replace personal identifiers with random values. Ex. 5 at 92:12-16, 116:15-19, 126:2-5, 127:14-19; JAF-19.

Watters. Watters's browsing history shows no instances of sensitive Etsy searches or URLs, and it is only *after* he joined this litigation that any URLs containing potential search terms appear in his browsing history. Exs. 25-27; JAF-10; JAF-17. Watters testified that he visits Etsy infrequently and is "not that concerned" about disclosing what items he is interested in. Ex. 7 at 65:22-66:9, 87:25-88:2 ("it is not a big deal to me"); JAF-14. Watters' browsing history shows no visits to Upwork or Sweetwater at all, let alone visits on which he entered sensitive, identifying search terms or visited URLs that revealed sensitive or identifying information. *See* Exs. 25-27; JAF-10; JAF-11; JAF-17. Watters testified that his only Upwork visits were perhaps in "early 2018 or sometime in mid-2020." Ex. 7 at 138:1-20; JAF-14. He cannot show the Pixel was installed on Upwork's website at the time of those visits or that any of his information was disclosed to Defendants—let alone that such information was sensitive and identifying. He never searched job listings in sensitive industries and never submitted any applications disclosing identifying information. Ex. 7. at 143:19-144:15, 148:4-18; JAF-14. Finally, Watters only made purchases as a guest on Sweetwater in "2019 or earlier,"

and he cannot show the Pixel was installed on Sweetwater's website at the time of those purchases or that any of his information was disclosed to Defendants—let alone that such information was sensitive and identifying. Ex. 7 at 160:2-14; JAF-14.

2. Plaintiffs have not shown that EAPI transmitted their identifying or sensitive information

There is no evidence that Defendants received any of Plaintiffs' data through EAPI. EAPI is a server-to-server connection between an advertiser and TTI that allows the advertiser to share event data with TTI, including those occurring on the advertiser's website. Ex. 28 ¶¶ 57-58. As with the Pixel, Plaintiffs have not offered any evidence that EAPI transmitted *sensitive, identifying* information about them to Defendants. Indeed, as demonstrated above, there is no sensitive or identifying information based on Plaintiffs' web browsing that even *could* have been available for EAPI to transmit to Defendants. Ex. 29 ¶¶ 17-19, 80-87. And Plaintiffs have not identified any events data involving them that were disclosed to Defendants—much less any events data pertaining to sensitive sales in which Plaintiffs had a reasonable expectation of privacy. For the same reasons as for the Pixel, Plaintiffs cannot state any claim based on EAPI.

* * *

Plaintiffs have not shown, and cannot show, that private information about them was shared with Defendants—indeed, the evidence confirms that no sensitive or identifying information about Plaintiffs was received by the third-party advertisers or disclosed to Defendants. As a result, there is no genuine dispute that Defendants did not invade Plaintiffs' reasonable expectation of privacy in a manner that would be highly offensive to a reasonable person. Under similar circumstances when a plaintiff did "not allege that she disclosed any sensitive information to Defendant, much less identify any specific personal information she disclosed that implicates a protectable privacy interest," this Court held that plaintiff had therefore

"not identified any harm to her privacy." *Byars*, 2023 WL 2996686, at *3 (dismissing privacy and wiretapping claims). The same result obtains here.

B. PLAINTIFFS' POSITION: Defendants' Sample Data Provides Evidence of Their Collection of Identifying Private Information from Plaintiffs

1. Defendants Misstate Applicable Law

Personally Identifying: Defendants are wrong as a matter of law that information must be personally identifying in order to be private. To the contrary, "***information need not be personally identifying to be private***." *In re Google Referrer Header Priv. Litig.*, 465 F.Supp.3d 999, 1009-10 (N.D. Cal. 2020) (anonymized search terms sufficient to allege ECPA claim "regardless whether those communications reveal the user's identity" because there is "concrete privacy interest in communications . . . ***even if those communications cannot be linked to the user***" (emphasis added)).

In *Brown v. Google*, the court ruled at summary judgment that the plaintiffs could have a reasonable expectation of privacy even in "anonymous, aggregated data" because "the reason Google has access to their anonymous, aggregated data [wa]s through the collection and storage of information from users' private browsing history without consent." 685 F.Supp.3d 909, 924, 940 n.39 (N.D. Cal. 2023) (denying summary judgment as to invasion of privacy, intrusion upon seclusion, and CIPA claims). In *Wesch v. Yodlee, Inc*., the court likewise concluded that the plaintiffs could have a "reasonable expectation of privacy in anonymized, aggregated data," because "it would only take a few steps to identify the individual Plaintiffs." 2021 WL 1399291, at *3 (N.D. Cal. Feb. 16, 2021). In *In re Google RTB Consumer Priv. Litig.*, the court at class certification held that information like "the URL of the website or app visited by the user; the IP address; the publisher of the website or application visited; various location fields; device information; and detected language" is "personally identifying." 2024 WL 2242690, at *7, *9 (N.D. Cal. Apr. 4, 2024).

Nonetheless, Plaintiffs' expert Dr. Shafiq has found [redacted] Ex. 58 at ¶¶8-33; Ex. 66. If plaintiffs in *Brown* and *Wesch* have a reasonable expectation of privacy in anonymous and aggregated data, Plaintiffs here certainly have a reasonable expectation of privacy in data that can [redacted].

Sensitive: It is a jury question whether the data collected on Plaintiffs is sensitive, and Plaintiffs have proffered sufficient evidence to demonstrate a dispute on that issue. In *Brown*, the court held at summary judgment that "the data collected was at least disputably sensitive" where plaintiffs proffered evidence that "users go Incognito [on their browsers] to search on sensitive topics and so that browsing data ***may*** reveal their sexual orientation, political or religious views, or upcoming big purchases." 685 F.Supp.3d at 941 (emphasis added). Given the vast volume of data collected in *Brown*, plaintiffs were not required to proffer evidence that some specific percentage of the data collected by Google constituted potentially sensitive data. Nor were plaintiffs in *Brown* required to proffer direct evidence of sensitive browsing activity for any specific website. *Id.* at 941, 924 n.9. Here, the volume of data is similarly vast, *see* Ex. 57 at ¶20 [redacted]), and thus there is no requirement that Plaintiffs proffer direct evidence of sensitive browsing activity. [redacted]

2. Sample Data from Defendants' Own Servers Provides Sufficient Evidence to Defeat Summary Judgment.

Defendants' two-day sample data contains evidence of [redacted]

[redacted] This is a tiny fraction of the data that Defendants collected on Plaintiffs over the putative class period—the vast majority of which Defendants have spoliated. *See* Dkt. 206-1.[6]

[redacted]

[6] On September 26, 2024, Plaintiffs served their portion of the joint stipulation regarding Plaintiffs' motion for Rule 37(e)(1) measures on Defendants. Plaintiffs plan on filing this motion before this Court with a hearing date of October 25, 2024.

[redacted]

Ex. 58 at ¶¶12-30.

[redacted]

[7] While Dr. Shafiq used the March 28, 2024 and May 21, 2024 data from Defendants to constitute the universe of websites that use or have used the Pixel or EAPI, this approach is conservative and likely resulted in an underinclusive list because any websites that in the past used either Pixel or EAPI but no longer did so by those two dates in 2024 would not be reflected in the two-day sample data.

[redacted]

To the extent that Defendants argue that Plaintiffs must show sensitive data from exclusively hulu.com, etsy.com, riteaid.com, buildabear.com, and upwork.com, *see supra* at p.5 n.2, that argument fails for three reasons. ***First***, while Defendants observe that a motion for summary judgment is "framed by the allegations in the pleadings," the Second Amended Complaint ("SAC") pleaded that

[redacted]

[8] [redacted]

the Pixel and EAPI are installed on "[a]t least 500,000 non-TikTok websites . . . , thereby allowing Defendants to obtain Private Data from visitors of these non-TikTok websites." Dkt. 137 at ¶59. The SAC makes clear that Hulu, Etsy, Rite Aid, Upwork, and Build-a-Bear are nonexhaustive examples of websites that use the Pixel or EAPI. *Id.* at ¶67; *see id.* at ¶68 (identifying 11 other widely used websites that use Pixel and through which Defendants collect non-TikTok user data); *accord id.* at ¶¶1, 27, 38, 45. The SAC further made clear that Hulu, Etsy, Rite Aid, Upwork, and Build-a-Bear are not the only websites that Plaintiffs visited from which Defendants took their data. *See id.* at ¶¶108, 115, 118, 124, 131, 135. Defendants were thus on notice of Plaintiffs' "theory of liability" from the start, and Plaintiffs' allegation that Defendants collect data from non-TikTok users via hundreds of thousands of websites that use the Pixel or EAPI has "guide[d] the parties' discovery." *Comprehensive*, 690 F.Supp.3d at 1114. [redacted] Indeed, Defendants' wide scope of collection is a large part of the violation.

Second, even if Plaintiffs were required to adduce evidence of specific sensitive content from these five specific websites, Defendants spoliated all but two days' worth of data that they collected from non-TikTok users like Plaintiffs. *See generally* Dkt. 206-1. Given that Defendants themselves have spoliated and/or withheld evidence of data that they collected on Plaintiffs, they cannot now complain that plaintiffs cannot meet their evidentiary burden without that data. *See Google RTB*, 2024 WL 2242690, at *10 ("Google cannot refuse to produce RTB data about other putative class members and then argue that, without this data, plaintiffs cannot meet their commonality burden."); *id.* (rejecting Google's efforts to defeat a CIPA claim by pointing to absence of evidence and observing that "Google never produced

this information and in fact objected to plaintiffs asking for it. It cannot use the tactic both as a shield and a sword."); *see also* Dkt. 206-1.[9]

3. Defendants' Caselaw Is Unavailing.

Defendants' cases are irrelevant. *Byars* is inapposite because the plaintiff there "d[id] not allege that she disclosed any sensitive information to Defendant," and there was no evidence that the plaintiff even engaged in the predicate activity at the root of her claims: communicate with defendant using its chat feature. 2023 WL 2996686, at *2-3. Here, by contrast, there is [redacted] *Hammerling* is also inapposite because the data collected there was "usage and engagement" data—*i.e.* metrics like what apps people installed and the amount of time spent on apps—but not the content of what people were doing on the apps. 615 F.Supp.3d at 1078. Here, by contrast, Plaintiffs have adduced undisputed evidence that [redacted] Ex. 30 at ¶¶57, 64-65, 78; JAF-45.

Nor does *Nickelodeon* help Defendants because the Third Circuit there limited its ruling to the Video Privacy Protection Act. 827 F.3d at 283-90. Indeed, the court heavily relied on the VPPA's legislative and post-enactment amendment history to hold that "static digital identifiers" do not constitute PII under VPPA and expressly distinguished other privacy statutes like the Children's Online Privacy Protection Act under which data like email address and telephone number do constitute "personal information." *Id.* at 286-87. Indeed, the *Nickelodeon* court reversed the district court's dismissal of the plaintiffs' intrusion upon seclusion claim under New

[9] While the two-day sample may not contain sensitive data about *Plaintiffs* from the hulu.com, etsy.com, riteaid.com, buildabear.com, and upwork.com, the sample does contain at least arguably sensitive data about putative class members from these websites. Ex. 58 at ¶48.

Jersey law as to one defendant. *See id.* at 293-95. More on point is *In re Google RTB*, in which the court recognized that "unique device identifier[s]" constitute "personal information" under California law. 606 F.Supp.3d 935, 944 (N.D. Cal. 2022).

IV. ISSUE NO. 2: INTERCEPTION

A. DEFENDANTS' POSITION: There is no evidence that Defendants intercepted the contents of Plaintiff's communications

Defendants are entitled to summary judgment on Plaintiffs' wiretapping claims (Counts 1 and 6) because there is no evidence that Defendants intercepted the contents of Plaintiffs' communications.

To state a claim under CIPA or ECPA, Plaintiff must allege that Defendants intercepted the contents of communications while "in transit" or contemporaneously used a device to record confidential communications. *See* Cal. Penal Code §§ 631, 632; *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) ("The analysis for a violation of CIPA is the same as that under the federal Wiretap Act."). For communications to be "intercepted," they "must be acquired during transmission, not while [they are] in electronic storage." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002). This is a "narrow definition" limited to "acquisition contemporaneous with transmission." *Id.*; *see also Flanagan v. Flanagan*, 41 P.3d 575, 581 (Cal. 2002) (drawing a "critical distinction between eavesdropping upon or recording a conversation and later disseminating its contents").

There is no evidence that Defendants' tools intercepted or recorded the contents of Plaintiffs' communications during transmission. And there is no genuine dispute that Plaintiffs' communications are not intercepted "in transit" or recorded when made.

1. The Pixel did not intercept the contents of Plaintiffs' communications

At the outset, Plaintiffs have not adduced evidence that the Pixel collected the contents of their communications. "[W]hether a URL constitutes 'contents'" of a communication subject to a reasonable expectation of privacy "turns on the specific

information Defendants obtain from each website that uses the Pixel." ECF No. 242 at 12; *see also Hammerling*, 615 F. Supp. 3d at 1092-93 (A full-string URL is not a communication's "content" unless it "reproduce[s] a person's personal search engine queries."). But Griffith and Shih, for example, [redacted] *See* Exs. 11-12, 21-24; JAF-34.

Beyond this threshold defect in those Plaintiffs' claims, there is no contemporaneous interception for *any* Plaintiff. Plaintiffs offer no evidence that the Pixel intercepted their communications "in transit" or simultaneously recorded those communications. To the contrary, the undisputed evidence shows that the Pixel operates *after* a user's communication with the website has already ended. *See* Ex. 28 ¶¶ 111-26; JAF-35. The Pixel sends data to Defendants from the *advertiser's* communication back to the browser, and not the *user's* communication to the website. *See* Ex. 28 ¶¶ 111-26; Ex. 4 at 192:18-193:21; Ex. 29 § VII.B; JAF-35. The Pixel does not intercept or record the *user's* communication to the website at all, let alone while it is "in transit" from the visitor to the website. *See id.*

As Plaintiffs' expert admitted, [redacted] Ex. 4 at 185:19-24; JAF-35. [redacted] Ex. 4 at 185:25-186:11; JAF-35. The undisputed evidence thus shows that the Pixel does not simultaneously intercept or record a search query as the user enters it; [redacted]. *See* Ex. 28 ¶¶ 111-26; Ex. 29 § VII.B JAF-35. This is the equivalent of interviewing a participant to a

conversation immediately after the fact, not eavesdropping on the conversation as it happens. *See Flanagan*, 41 P.3d at 581 (CIPA prohibits "simultaneous dissemination," not "secondhand repetition").

Finally, when a website uses "technology created by others" to collect communications, the company that created that technology is not the one intercepting communications. *Valenzuela v. Kroger Co.*, 2023 WL 4418887, at *3 (C.D. Cal. June 23, 2023). The evidence shows no interception here, but Defendants could not be responsible for the hypothesized interception in any event because they do not control how Rite Aid, Hulu, Etsy, Upwork, Build-A-Bear, or Sweetwater set up websites, configure their URLs, or operate the Pixel. *See* Ex. 28 ¶¶ 19, 40, 44-45, 57-59, 67, 80(a), (b), 111-126; Ex. 29 § VI.A; Ex. 3 at 142:13-144:1, 199:8-14, 209:3-14; JAF-35.

2. EAPI did not intercept the contents of Plaintiffs' communications

As the Court has already recognized, "Events API sends information directly from the [advertiser] third party's server to Defendants' server without involving the browser in the communication." ECF No. 242 at 2. That fact is dispositive. Indeed, Plaintiffs' own expert testified that EAPI "is implemented in such a way that information that is collected from a user's browser is first sent to a server, and from that server, the information is relayed to TikTok's server." Ex. 4 at 122:14-20; *see also* Ex. 28 ¶¶ 57-60; Ex. 29 ¶¶ 112-114; JAF-37; JAF-38. Definitionally, that is not interception. *See Konop*, 302 F.3d at 878.

B. PLAINTIFFS' POSITION: Factual Disputes on "Contents" and "Interception" Preclude Summary Judgment.

Plaintiffs have established triable issues of fact that Defendants contemporaneously "intercept" the "contents" of communications.

1. "Contents"

Defendants misread *Hammerling* to suggest that a URL must contain search terms to constitute "contents." To the contrary, "ECPA broadly defines 'content' as

that which 'includes any information relating to the substance, purport, or meaning' of the communication at issue." *Google RTB*, 606 F.Supp.3d at 949 (holding ECPA "contents" include "URL of the page where the impression will be shown" and "referrer URL that caused navigation to the current page"). In *Brown*, the court held at summary judgment that "https%3A%2Fwww.washingtonpost.com%2Fworld%2F2022%2F02%2F18%2Frussia-ukraineupdates%2l"—a URL with no search term—could constitute "contents" under ECPA "by virtue of including the particular document within a website that a person views," which "divulge[s] a user's personal interests, queries, and habits." 685 F.Supp.3d at 935 (citation omitted); *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008); *In re Meta Pixel Healthcare Litig.*, 647 F.Supp.3d 778, 796 & n.10 (N.D. Cal. 2022) (URLs like https://www.medstarhealth.org/doctors/paul-a-sack-md that include the "path" are "content because they concern the substance of a communication").

[redacted]

[redacted] While the URLs alone are sufficient to survive summary judgment, Dr. Shafiq also described two other categories of data—Event Information and Content Information—that constitute "contents" under CIPA and ECPA. *See* Ex. 30 at ¶¶57, 64-65, 78; JAF-45.

2. "Interception"

Pixel: To argue that they do not "intercept" Plaintiffs' data, Defendants put arbitrary limits on the definition of "communications" that find no support in fact or law. First, Defendants try to distinguish between the "*user's* communication" (search term) and the "*advertiser's* communication" (search results) to argue that interception of the latter does not count. They cite no authority for this proposition—because it plainly contradicts California law. In *Gruber v. Yelp, Inc.*, 55 Cal.App.5th 591 (Cal. App. 2020), the court rejected Yelp's efforts to distinguish between the communications of a consumer and those of a call center representative and ruled that even a one-way recording of only the representative's end of a call (without recording the consumer's voice) constitutes a CIPA violation: "[T]he term 'communication' for purposes of CIPA connotes a singular conversation or exchange shared between two or more participants. . . . [CIPA] make[s] no distinction between the speaker and the listener or between the caller and the call recipient. Rather, all are equally referred to as 'parties.'" *Id.* at 607. So too here. TikTok's admitted interception of the advertiser's communication (search results returned in response to search terms) constitutes CIPA interception.

Second, Defendants try to limit the type of communication at issue to only search terms and results, which ignores all the other data that Pixel collects immediately as soon as a non-TikTok user visits a website. Dr. Shafiq has found that [redacted]

[redacted] Ex. 30 at ¶¶57, 64-65, 78; JAF-45. [redacted] Ex. 68 at TIKTOK-BG-000008586; Ex. 69 at TIKTOK-BG-000151817; Ex. 65 (143:9-19); Ex.30 at ¶70; JAF-39. There is at least a triable issue of whether TikTok intercepts these other contents.

Finally, even if, contrary to the law, [redacted]. Ex. 58 at ¶¶55-56; JAF-46. A reasonable juror could disregard such hair-splitting and [redacted]. *See United States v. Szymuszkiewicz*, 622 F.3d 701, 706 (7th Cir. 2010), *as amended* (Nov. 29, 2010) (rejecting argument that "contemporaneous" must mean "in the middle" for ECPA, and noting that if two persons communicating were "sitting at their computers at the same time, they would have received each message with ***no more than an eyeblink in between. That's contemporaneous by any standard***." (emphasis added)).

The contemporaneousness here is unlike those in Defendants' cases, where significant time had elapsed between the communication and interception. *See Flanagan*, 27 Cal.4th at 770-71 (defendant installed voice-activated tape recorder to record telephone calls and played the tapes later); *Konop*, 302 F.3d at 878 (defendant-employer accessed plaintiff-employee's website and read previously written posts). *Valenzuela*, 2023 WL 4418887, at *3, is also inapposite: Unlike plaintiff there who had not identified any third party that intercepted her communication with Kroger's chatbot, here Defendants themselves are the third party that intercepts communications.

EAPI: [redacted] Ex. 70 (emphasis in original); Ex. 56 ¶102; JAF-41. Defendants have provided no specific examples of websites disregarding this directive. TikTok's own documents create at least a factual dispute as to whether real-time transmission of data from browser to advertiser's server to TikTok can constitute a contemporaneous interception.

V. ISSUE NO. 3: CONSENT

A. DEFENDANTS' POSITION: Plaintiffs consented to advertisers' use of the Pixel and EAPI.

Defendants are entitled to summary judgment on *all of* Plaintiffs' claims because Plaintiffs consented to sharing their data with third parties such as Defendants. Lack of consent is an element of Plaintiffs' CIPA claim, *see* Cal. Penal Code § 632(a), and consent is a defense to Plaintiffs' other claims, *see Calhoun v. Google LLC*, 526 F.Supp.3d 605, 619 (N.D. Cal. 2021) (collecting statutory provisions and cases). Consent "can be explicit or implied, but any consent must be actual." *Id.* at 620 (quotation omitted). The undisputed facts show that Plaintiffs manifested both express and implied consent to advertisers' use of Defendants' Pixel and EAPI.

1. Plaintiffs expressly consented when they created accounts

Plaintiffs created accounts on Rite Aid (Griffith), Hulu (Griffith, Shih), Etsy (Griffith, Shih, Watters), and Upwork (Shih, Watters),[10] and agreed to those sites' privacy policies, thereby expressly consenting to disclosure of their data to third parties such as Defendants.

[10] Watters has adduced no evidence that the Pixel was installed on Sweetwater's website when he made purchases, and any subsequent browsing could not have transmitted identifying information to Defendants because he was not signed in.

"[I]nternet contracts are classified by the way in which the user purportedly gives their assent to be bound by the associated terms: browsewraps, clickwraps, scrollwraps, and sign-in wraps." *Keebaugh v. Warner Bros. Ent. Inc.*, 100 F.4th 1005, 1014 (9th Cir. 2024) (quotation omitted). A clickwrap agreement "requires users to click on an 'I agree' box after being presented with a list of terms and conditions of use." *Id.* "Courts have routinely found clickwrap agreements enforceable." *Id.* (quotation omitted). A "sign-in wrap agreement" advises that by clicking "Sign in," "Create my account," or something similar, the user agrees to the website's terms. *See id.* Sign-in-wrap agreements are enforceable if the user has actual knowledge of the agreement or if "(1) the website provides reasonably conspicuous notice of the terms to which the consumer will be bound; and (2) the consumer takes some action, such as clicking a button or checking a box, that unambiguously manifests his or her assent to those terms." *Id.* (quotation omitted).

Under similar circumstances as these, courts have rejected privacy and wiretapping claims based on users' express consent to terms. *See, e.g.*, *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 953-56 (N.D. Cal. 2017), *aff'd*, 745 F. App'x 8 (9th Cir. 2018); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1021 (N.D. Cal. 2014).

a) Rite Aid

Griffith cannot state a claim based on her visits to Rite Aid's website because she agreed to its Privacy Policy, which disclosed that Rite Aid would "share personal information with third parties," including through "pixel tags."

For several years, beneath Rite Aid's "Create Account" button is the admonition: "By clicking created account, you acknowledge you have read and agree to Rite Aid[']s Terms of Use and Privacy Policy"—each of which is hyperlinked. Ex. 32; *see also* Ex. 33 (substantially similar); JAF-47. Griffith estimates a half-dozen visits to Rite Aid's website in the last two or three years, though she cannot recall when she created her Rite Aid account. *See* Ex. 2 at 68:21-69:11, 219:22-220:7; JAF-47. Griffith was also aware from her personal experience

that privacy policies disclose that websites share her data with third parties. Ex. 2 at 132:8-11; JAF-47.

Since at least March 2018, Rite Aid's Privacy Policy has disclosed that it "collect[s] personal information you provide when using the Riteaid.com website" including specific "personally identifiable information," as well as "information about your viewing, search and purchase history and information about the referring URL and the URL clickstream to, through, and from our Site." Ex. 45 ("What Information We Collect"; "Information Automatically Collected"); JAF-28. Rite Aid further disclosed that it would "share personal information with third parties who perform services on our behalf. Ex. 45 ("How We Use Your Information"); JAF-48. Rite Aid reserved its right to amend the Privacy Policy, JAF-47, and later amendments added even more detailed disclosures, such as that Rite Aid may deploy "pixel tags … and similar technology" and may use "other advertising techniques to share limited identifying information including Online User Activity with advertising partners," Ex. 34 §§ 10(A)(1), 1(D); JAF-49.

b) Hulu

Neither Griffith nor Shih can state a claim based on their visits to Hulu because they accepted its Privacy Policy, which contains similar disclosures about data-sharing.

Between 2010 and 2012, Hulu used both clickwrap and sign-in-wrap agreements. *See* Ex. 46; Ex. 47; JAF-51. In 2010, users were required to check a box indicating "I agree to the Terms of Use and Privacy Policy." Ex. 46; JAF-31. By January 2012, users were notified above a "Sign Up" button that "By clicking Sign Up, you are indicating that you have read and agree to the **Terms of Use** and **Privacy Policy**"—both hyperlinked. Ex. 47; JAF-51.

Shih created her only Hulu account in July 2011 and ended her subscription in 2013—years before the Pixel or EAPI was introduced. *See* Ex. 18 at 1; Ex. 5 at 205:13-206:14; JAF-51. Hulu's Privacy Policy disclosed that "information about

you is collected, used and shared," including through "cookies, web beacons or other technologies." Ex. 37 ("Information Collected About You" and "Third Party Advertising On Hulu"); JAF-52. These "other technologies" included "pixel tags," and Hulu would "share your information with companies that provide … advertising." *Id.* Further, Hulu partners with "third party Internet advertising companies" that "use cookies, web beacons, and other technologies to collect information about your use of the Hulu Services in order to deliver advertisements to you, measure their effectiveness, and personalize advertising content." *Id.*

Griffith created Hulu accounts in February 2019, November 2020, April 2023, and November 2023. *See* Ex. 13 at 1; Ex. 14 at 1; Ex. 15 at 1; Ex. 16 at 1; JAF-50. Between 2018 and 2020, Hulu users were presented with a "Continue" button, above which reads "By clicking 'Continue,' you agree to our Hulu Terms of Use and Privacy Policy"—each of which was hyperlinked. Ex. 35 at 1; Ex. 36 at 1; JAF-50. The account-creation page in 2023 was materially similar. Ex. 48 at 1; JAF-50.

At all relevant times for Griffith, Hulu's Privacy Policy disclosed that it collects "information you provide to us" including, inter alia, "information about the videos you view on Hulu (e.g., show titles and episode names), page views, ad data, referral URLs, network state, device identifiers or other unique identifiers such as advertising identifiers … and identifiers associated with browser cookies." Ex. 38 §§ 2, 4; Ex. 39 §§ 2, 4; *see also* Ex. 40 ("Types of Information We Collect"); JAF-53. Hulu specifically disclosed its use "cookies" and "web beacons or pixel tags, which can be embedded in web pages, videos, or emails, to collect certain types of information from your browser or device." Ex. 38 § 2; Ex. 39 § 2; *see also* Ex. 40 ("How We Collect Your Information"); JAF-54. Finally, Hulu would "share information collected from or about you with third parties … , including business partners," including for advertising purposes. Ex. 38 §§ 2, 4; Ex. 39 §§ 2, 4; *see also* Ex. 40 ("Use Of Your Information By The Walt Disney Family Of Companies"; "Sharing Your Information With Other Entities"); JAF-53. It warned: "**If you do**

not consent to the collection and use of information from or about you in accordance with this Privacy Policy, then you may not use the Hulu Services." Ex. 38 § 1 (emphasis in original); JAF-50.

c) Etsy

Shih, Griffith, and Watters cannot state a claim based on their visits to Etsy because they accepted its Privacy Policy, which also disclosed data-sharing.

Shih and Griffith. Shih created an Etsy account in June 2017 and Griffith created one in June 2018. *See* Ex. 9; Ex. 17; JAF-35; JAF-56. In 2017 and 2018, users creating Etsy accounts were presented with a "Register" button, below which was the admonition: "By clicking 'Register,' you agree to Etsy's Terms of Use and Privacy Policy"—both of which were hyperlinked. Ex. 50; Ex. 51; JAF-55; JAF-56.

In June 2017, Etsy's Privacy Policy explained that "[b]y visiting the Site or using the Apps, you consent to our collection, transfer, manipulation, storage, disclosure and other uses of your information as described in this policy. This includes any information you choose to provide that is deemed sensitive under applicable law." Ex. 41; JAF-56. It further disclosed that, among the ways it would share that data, was "work[ing] with certain third-party service providers for targeted online and offline marketing." Ex. 41 ("Information Collected or Received"); JAF-38. Etsy disclosed it would collect "your IP address or unique device identifier, cookies and data about which pages you visit on the Site or on the Apps and stores it in log files" and "combine this automatically collected information with other information we collect about you." *Id.* Further, "certain cookies and other tracking mechanisms on our site are used by third parties for targeted online marketing and other purposes." Ex. 41 ("Information Uses, Sharing & Disclosure"); JAF-59. Etsy's May 2018 update added that "If you don't want us to collect or process your personal information in the ways described in this policy, you shouldn't use the Services." Ex. 52; JAF-60.

Watters. Watters signed up in December 2020, and specifically remembered agreeing to Etsy's terms and conditions. *See* Ex. 7 at 66:17-24, 76:5-25; JAF-57. At that time, beneath the "Sign in" button was the admonition: "By clicking Sign in or Continue with Google, Facebook, or Apple, you agree to Etsy's Terms of Use and Privacy Policy"—both hyperlinked. Ex. 49; JAF-57. The December 2020 version of the Privacy Policy contained materially similar disclosures to those above. Ex. 53 §§ 2, 6; JAF-61; JAF-62.

d) Upwork

Shih and Watters cannot state a claim based on their visits to Upwork because they accepted Upwork's Privacy Policy, which likewise disclosed data-sharing. Users creating an Upwork account must check a box stating "Yes, I understand and agree to the Upwork Terms of Service, including the User Agreement and Privacy Policy"—each of which is hyperlinked. Ex. 42; JAF-63; JAF-64.[11]

By creating accounts, Shih and Watters agreed to Upwork's terms and consented to data-sharing with third parties. Watters created an Upwork account in "early 2018." *See* Ex. 7 at 138:1-139:11; JAF-64. Shih created an Upwork account on March 9, 2022. *See* Ex. 19; JAF-63. She was later notified by email about a Privacy Policy update on November 26, 2023, which contained even more extensive disclosures. *See* Ex. 20; JAF-63. She also testified that she would review privacy policies to sign-up for websites and would click a checkbox agreeing to terms when required to do so for sign-up. Ex. 5 at 162:5-165:4; JAF-63.

In early 2018, Upwork's Privacy Policy disclosed its collection of "information that identifies you as a specific individual and can be used to contact or identify you," such as "your name, email address, company address, billing

[11] The Internet Archive's Wayback Machine does not appear to have captured functional versions of Upwork's sign-up page in 2018. Ex. 31 ¶ 16. And although it captured Upwork's initial sign-up screen in March 2022, it does not appear to have captured the full sign-up process occurring on the screen after a user enters her email address. *Id.*

address, and phone number." Ex. 43 § 1; JAF-66. Upwork explained that it also "may render Personal Information (generally, email address) into a form of Non-Identifying Information referred to … as 'Hashed Information'" and share that information with "third parties." Ex. 43 § 1; JAF-67.

Upwork notified users that "[w]e and our third party service providers, including analytics and third party content providers, may automatically collect certain information from you whenever you access or interact with the Service," including:

> the browser and operating system you are using, the URL or advertisement that referred you to the Service, the search terms you entered into a search engine that led you to the Service, areas within the Service that you visited, and other information commonly shared when browsers communicate with websites. We may combine this automatically collected log information with other information we collect about you.

Ex. 43 § 1; JAF-69. Among other things, Upwork disclosed the use of "both persistent cookies that remain on your computer … and session ID cookies, which expire at the end of your browser session," as well as "software technology known as 'web beacons' and/or 'tracking tags' … to serve relevant advertising to you." Ex. 43 § 1; JAF-65.

Finally, Upwork disclosed that it "works with (or may in the future work with) network advertisers, ad agencies, analytics service providers and other vendors to provide us with information regarding traffic on the Service," and that these third parties "may collect certain information about your visits to and activity on the Service as well as other websites or services, they may set and access their own tracking technologies on your device (including cookies and web beacons), and may use that information to show you targeted advertisements." Ex. 43 § 1; JAF-70.

Upwork's 2022 Privacy Policy contained materially similar disclosures. Ex. 54 §§ 1, 4, 5; JAF-71 through JAF-76.

2. Plaintiffs impliedly consented by conduct

In addition to these numerous explicit consents, Plaintiffs also impliedly consented to use of Defendants' Pixel and EAPI through their course of conduct.

Implied consent may be "inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance." *Berry v. Funk*, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (applying ECPA) (cleaned up). "The key question in such an inquiry obviously is whether parties were given sufficient notice." *Id.* To maintain a claim for invasion of privacy, a plaintiff "must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant." *Hill v. Nat'l Collegiate Athletic Ass'n.*, 865 P.2d 633, 648 (Cal. 1994). When a party knows that activity is monitored, continued activity manifests consent. *Berry*, 146 F.3d at 1011 (citing *Griggs-Ryan v. Smith*, 904 F.2d 112, 118 (1st Cir. 1990)); *see also Rojas v. HSBC Card Servs. Inc.*, 93 Cal. App. 5th 860, 886 (2023) (applying *Berry* and *Griggs-Ryan* to CIPA).

Continuing to use an advertiser's website despite knowing that it collects and shares browsing information is not "consistent with an actual expectation of privacy." *Hill*, 865 P.2d at 648. And it is undisputed here that Plaintiffs continue to use websites despite their actual knowledge of advertisers' use of the Pixel and EAPI and disclosure of data to Defendants. For example, *after filing this suit* and despite knowing Hulu uses the Pixel, Griffith created a new Hulu account. *See* Ex. 13 at 1; Ex. 2 at 176:18-20; JAF-77. And her browsing history shows that she also visited the Etsy, Hulu, and Build-A-Bear websites after she initiated this litigation. Ex. 12; JAF-77. Shih investigated whether the websites she visited used the Pixel and nevertheless continued to visit the websites she believes use the Pixel or EAPI. *See* Ex. 5 at 264:6-276:9, 280:12-282:14; JAF-78. In fact, she continues to use Upwork despite its deployment of the Pixel. Ex. 5 at 293:10-13; JAF-78. Similarly, even after joining this litigation, Watters continues to visit Etsy. *See* Exs. 25-26; JAF-79.

Plaintiffs' continued use of advertisers' websites—even after learning about their use of the Pixel and, as appliable, EAPI—is thus further a manifestation of consent.

B. PLAINTIFFS' POSITION: A Reasonable Juror Could Find There Was No Consent.

There are material disputes over consent. Except as to the CIPA § 632(a) claim, consent is "an affirmative defense for which defendant bears the burden of proof." *Calhoun v. Google, LLC*, 113 F.4th 1141, 1147 (9th Cir. 2024) (quoting *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1044 (9th Cir. 2017)). In determining consent, courts consider "whether the circumstances, considered as a whole, demonstrate that a reasonable person understood that an action would be carried out so that their acquiescence demonstrates knowing authorization." *Id*. (quoting *Smith v. Facebook, Inc*. 745 F.App'x 8, 8 (9th Cir. 2018)).

Denying Defendants' motion to dismiss, this Court already ruled that Defendants did not establish a consent defense because "it is undisputed that the privacy policies ***generally disclosed*** that some of Plaintiff's information would be shared with third parties ***but did not specifically provide that it would be given to TikTok (even when providing detailed lists of other third-parties whose cookies were present on the websites)***." *Griffith v. TikTok, Inc*., 697 F.Supp.3d 963, 972 (N.D. Cal. 2023) (emphasis added). This is law of the case. *See United States v. Alexander*, 106 F.3d 874, 876 (9th Cir. 1997) ("Under the 'law of the case' doctrine, 'a court is generally precluded from reconsidering an issue that has already been decided by the same court, or a higher court in the identical case.'" (citation omitted)). Even if the Court were to revisit the same privacy policies that it already ruled inadequately disclosed Defendants' data collection, Defendants have not met their burden to establish no material dispute as to consent.

1. No Express Consent

"[C]onsent "can be express or implied, but any consent must be actual." *Calhoun*, 113 F.4th at 1147 (cleaned up). "For consent to be actual, the disclosures must 'explicitly notify' users of the conduct at issue." *Id.* (citations omitted). "Generalized notice," such as in the privacy policies of websites visited by Plaintiffs that don't mention Defendants or the Pixel or EAPI specifically, "is not sufficient to establish consent." *Meta Pixel*, 647 F.Supp.3d at 793. Summary judgment on issues of express consent must be denied unless the terms of a privacy policy are "unambiguous[]," *see Brown*, 685 F.Supp.3d at 928, and "explicitly address" a defendant's conduct, *Opperman v. Path*, 205 F.Supp.3d 1064, 1074 (N.D. Cal. 2016). Similarly, summary judgment should be denied where language is "susceptible to more than one reasonable interpretation." *Digital Envoy, Inc. v. Google, Inc.*, 370 F.Supp.2d 1025, 1033 (N.D. Cal. 2005). Consent "to a particular data collection practice is not to be determined by attributing to that user the skill of an experienced business lawyer or someone who is able to easily ferret through a labyrinth of legal jargon to understand what he or she is consenting to." *Calhoun*, 113 F.4th at 1151. Defendants fail to meet these high standards.

a) No Privacy Policy Mentions Defendants

No privacy policy cited by Defendants mentions TikTok or ByteDance. At minimum, this absence creates a disputed issue of fact as to whether the policies "explicitly address" the conduct in question, *Opperman*, 205 F.Supp.3d 1064, and whether a "reasonable user" would have understood that ***Defendants*** were taking their data, *Calhoun*, 113 F.4th at 1151.

Further, the omission of any reference to TikTok and ByteDance is all the more glaring when juxtaposed with the fact that several of the privacy policies cited by Defendants specifically mention by name other social media platforms:

- Hulu specifically mentions Facebook as a "Social Networking Service[]." Ex. 37, 38.

- Etsy specifically mentions Facebook as a third-party application. Ex. 41.
- Upwork specifically names Facebook and LinkedIn as third-party services that integrate in the Upwork site. Ex. 43.

Given the explicit naming of other companies but not Defendants, there is at least a factual dispute as to whether a "reasonable user" would have understood these websites to be sharing data with Defendants. *Calhoun*, 113 F.4th at 1150-51. Indeed, at deposition, Jacob Watters, when asked to review language in an Etsy privacy policy, noted that "I don't know what advertising or marketing providers are currently -- ***they only explicitly list Facebook and Google.*** Those are the only two third parties that I can definitively say that I know my data has been shared with." Ex. 7 (100:7-11) (emphasis added).

b) The Privacy Policy Disclosures About Data Collection Are Generalized and Ambiguous

The language in privacy policies cited by Defendants is too ambiguous and generalized to manifest Plaintiffs' consent as a matter of law. For example, the privacy policies discuss third parties such as "advertising partners" or "analytics" providers. However, Plaintiffs, or any reasonable user, would have no reason to believe that Defendants would fall into one of these categories. TikTok presents itself as a social media or video sharing platform, not an advertising service or analytics platform. In fact, TikTok, on its "About" page, describes itself as "the leading destination for short-form mobile video." Ex. 76. For non-TikTok users, there is doubly no reason to think of TikTok in the context of advertising or analytics, as they are not served advertisements by TikTok nor would they be part of the TikTok platform's analytics.

i. Rite Aid

One of Rite Aid's privacy policies, cited by Defendants, stated that Rite Aid would "share personal information ***with third parties who perform services on our behalf***." Ex. 45 (emphasis added). There is at least a genuine dispute as to whether

this definition of "third party" puts Plaintiffs on notice of collection of personal data by Defendants and whether a reasonable user would suspect that a social-media platform would be a service performer for Rite Aid.

Defendants also note that the policy stated that Rite Aid collects "personally identifiable information." Ex 45. However, the policy stated that "this information is necessary, for example, to respond to your questions, provide your additional healthcare information and coupons or process your order." *Id*. None of the usages listed by Rite Aid includes the function of the Pixel or EAPI.

Similarly, as noted by Defendants, that policy also stated that "***We*** automatically receive and collect certain types of information . . . This information about your viewing, search and purchase history, and information about the referring URL and the URL clickstream to, through, and from our Site." (Emphasis added.) This language puts a reasonable user on notice that Rite Aid ***itself*** receives and collects the information at issue; it makes no mention of any third party's involvement.

Similarly, Defendants cite to language in a Rite Aid policy from another date that states that it uses "other advertising techniques to share limited identifying information including Online User Activity ***with advertising partners***," Ex. 34 (emphasis added). However, as stated above, there is at least a factual dispute as to whether a non-TikTok user would have any notice of, or reason to know, that TikTok is an "advertising partner" in this regard.

ii. Hulu

In a Hulu privacy policy cited by Defendants, Hulu states: "***We*** collect information when you use the Hulu Services or view Hulu advertising outside the Hulu Services. Examples of this information may include" various data categories. Ex. 38 (emphasis added). This paragraph states that Hulu ***itself*** collects this data and makes no mention of a third party's involvement.

Similarly, that same policy states that:

> We may share the information collected from or about you in ***encrypted, aggregated, or de-identified forms*** with advertisers and service provides that preform advertising-related services for us and our business partners in order to tailor, advertisements, measure and improve advertising effectiveness, and enable other enhancements.

Ex. 38 (emphasis added). Given that the sharing disclosed here would be in encrypted, aggregated, or de-identified forms only, this would specifically ***exclude*** sharing via Pixel and EAPI, which the two-day sample [redacted]

Hulu states in a policy with a different date that it may share data with "third party Internet advertising companies" that "***in order to deliver advertisements to you, measure their effectiveness, and personalize advertising content.***" Ex. 37 (emphasis added). Again, there is at least a disputed issue whether non-TikTok users who are not served ads on the TikTok platform had any reason to suspect that Defendants might fall into this category.

Similarly, the policy noted that "[w]e also may use services that collect data remotely by using so-called 'pixel tags.'" *Id.* However, the use of the term "services" is vague and overbroad, there is no explanation of what it means to "collect data remotely" or what a "pixel tag" is or does, and there is no disclosure to suggest that Defendants may be one of these services.

iii. Etsy

An Etsy privacy policy, cited by Defendants, states that Etsy was "work[ing] with certain third-party service providers for ***targeted online and offline marketing***." Ex. 41. Again, it is at minimum a disputed fact whether reasonable users, particularly non-TikTok users, would understand this language to disclose Defendants' involvement.

This policy also notes that "***Etsy*** automatically receives and records information from your browser or your mobile device when you visit the Site or use the Apps, such as" various sensitive data. *Id.* (emphasis added). In this disclosure, it only states that "Etsy" ***itself*** collects this data, and makes no mention of any third

party's involvement. Again, all this sentence says is that Etsy itself, not any third party, collects this data.

iv. Upwork

Upwork's privacy policy states that:

> We and our ***third party service providers, including analytics and third party content providers,*** may automatically collect certain information from you whenever you access or interact with the Service. This may include, among other information, [various data categories]. We may combine this automatically collected log information with other information we collect about you. We do this ***to improve services we offer to you, to improve marketing, analytics, and site functionality***.

Ex. 43 (emphasis added). Similarly, Upwork states that it "[w]orks with (or may in the future work with) ***network advertisers, ad agencies, analytics service providers*** and other vendors to provide us with information regarding traffic on the Service, including pages viewed and the actions taken when visiting the Service" and that the third parties "may use that information to ***show you targeted advertisements***." *Id*. (emphasis added). As discussed above, this language does not establish consent as a matter of law because TikTok presents itself to the public as a social media or video sharing platform, not a third party "service provider," "analytics" provider, or "content provider."

In other language cited by Defendants, Upwork states that it collects "information that identifies you as a specific individual and can be used to contact or identify you," and mentions various data categories. *Id.* In context, however, the paragraph limits the collection of this information specifically to Upwork for the purpose of contacting or identifying its users; there is no mention that such information will be shared with third parties.

Similarly, Defendants cite to language in this policy stating that Upwork or marketing affiliates, analytics, and service providers use "both persistent cookies that remain on your computer . . . and session ID cookies," as well as the use "web beacons" and/or "tracking tags." *Id*. As stated above, there is at least a dispute as to whether a reasonable user would consider Defendants to be "marketing affiliate[s]"

or analytics or service providers, especially when Defendants are not disclosed by name and where the visitor reading the policy is not a TikTok user.

Finally, Defendants' write: "Upwork explained that it also 'may render Personal Information (generally, email address) into a form of Non-Identifying Information referred to … as "Hashed Information"' and share that information with 'third parties.'" [redacted] Ex. 58 at ¶47, Ex. 72. There is at least a disputed issue whether a reasonable user reading the Upwork policy would have been on notice of [redacted] Ex. 58 at p.4, n.6.

v. Other Websites

Defendants discuss the privacy policies of four websites only, and not those of any others that Plaintiffs visited that use the Pixel or EAPI. *See supra* Sec. III.B.2; Exs. 66-67. This is a glaring omission that precludes summary judgment in Defendants' favor given that the four websites Defendants focus on are only "representative examples" of non-TikTok websites visited by Plaintiffs. *See* Dkt. 137 at ¶¶115, 124, 135; *see also* Ex. 57 at ¶¶22, 109 ([redacted]).

2. No Implied Consent

Defendants' argument that Plaintiffs' continued visits to these four websites after litigation manifests implied consent is foreclosed by law. In *Rodriguez v, Google LLC*, 2024 WL 38302 (N.D. Cal. Jan. 3. 2024), the court, over Google's consent defense, certified classes of millions of Google users who had Google's

"Web & App Activity" setting turned off. The court held that "it is unreasonable" to expect, and it is an "undue burden" for, consumers to stop using apps with Google SDKs "to show a lack of consent." *Id.* at *5; *cf. In re Yahoo Mail Litig.*, 308 F.R.D. 577, 589 (N.D. Cal. 2015) (rejecting Yahoo's argument that plaintiffs manifested consent by continuing to email Yahoo Mail subscribers after litigation because accepting such argument would place "impossible burden" on plaintiffs and place them in a "catch-22" where they would have to simultaneously stop emailing Yahoo subscribers to avoid consent while continuing to email Yahoo subscribers to prove injury). Given that these four websites are not the only ones that use the Pixel or EAPI and that Plaintiffs cannot even know the full universe of websites that use these trackers, Defendants are essentially arguing that Plaintiffs stay off the internet altogether to avoid consenting to Defendants' data-harvesting campaign. The court should not place such an "undue," "impossible" burden on Plaintiffs.

Relatedly, even if Plaintiffs had impliedly consented with respect to those four websites, which they did not, Defendants have introduced no evidence that Plaintiffs impliedly consented to any other website they visited which contained the Pixel or EAPI. And with respect to the four websites identified by Defendants, even assuming implied consent after the date of commencement of litigation, such implied consent is not retroactive to Defendants' unlawful activities before the litigation. *See, e.g., Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *2 (9th Cir. May 31, 2022) (retroactive consent insufficient to defeat CIPA claim).

Defendants also ignore record evidence from Plaintiffs' declarations and deposition testimony making clear that they did not consent to Defendants' data collection. *See* Ex. 7 (345:17, 233:10-14); Ex. 5 (282:13-14, 346:1-347:1); Exs. 73-75, ¶6.

Defendants' cases do not establish implied consent in the instant context. The court in *Griggs–Ryan v. Smith*, 904 F.2d 112, 118 (1st Cir.1990), found implied consent where a prison inmate was "told unequivocally that all incoming calls would

be recorded." If anything, *Berry v. Funk*, 146 F.3d 1003, 1011 (D.C. Cir. 1998), in which the court ***denied*** summary judgment on the implied consent issue, reaffirms how fact-intensive this inquiry is. *See id.* at 1011 (noting factual dispute as to whether "an operator's failure to inform a party that he is getting off the line normally raises a suspicion in a reasonable person's mind that his call is being monitored"). And *Hill v. Nat'l Collegiate Athletic Ass'n.*, 865 P.2d 633, 648 (Cal. 1994), did not involve implied consent at all.

VI. ISSUE NO. 4: PROPERTY

A. DEFENDANTS' POSITION: There is no evidence that Defendants took Plaintiffs' property

Defendants are entitled to summary judgment on Plaintiffs' property claims (Counts 2 and 3) because there is no evidence that Defendants took Plaintiffs' property. As this Court explained, "whether [Plaintiffs] have a cognizable property interest in the information sent to defendants … turns on the nature of that information and whether it carries financial value." ECF No. 242 at 11. Here, Plaintiffs have failed to adduce evidence of what (if anything) was purportedly taken, let alone that it had marketable value and was exclusively theirs.

There is no evidence that a user—like Plaintiffs—"who briefly visits a few websites using the Pixel and shares no sensitive information has a marketable property interest in the data collected by the websites." *Id.* For similar reasons, Plaintiffs have not offered evidence that, if Defendants collected a copy of their information, Plaintiffs somehow lost property as a result. After all, even if "a plaintiff's information is valuable in the abstract, and simply because a company might have made money from it, that does not mean that the plaintiff has 'lost money or property as a result.'" *Doe I v. Google LLC*, 2024 WL 3490744, at *7 (N.D. Cal. July 22, 2024) (citation omitted).

Plaintiffs' own testimony shows their understanding that they did not lose valuable money or property. Griffith, for example, testified that she has never

attempted to sell her website event data. Ex. 2 at 238:22-239:2; JAF-93. Shih testified that she had not attempted "selling my own data" because she "d[id]n't think there is a market." Ex. 5 at 334:19-335:21; JAF-93. She had also never attempted to sell or monetize her hashed PII. Ex. 5 at 338:19-341:7; JAF-93. Watters testified that although he had attempted to monetize his participation in surveys, he never "buil[t] up enough of [website] currency to be able to cash anything out" and had "not been allowed meaningful participation that would allow [him] to be compensated for [his] time at a reasonable rate." Ex. 7 at 257:25-261:3; JAF-93.

Furthermore, even if the data had marketable value, Plaintiffs have not adduced evidence that they exercised exclusive control over whatever information they allege was collected from them. A property right exists only if it is "capable of exclusive possession or control" and "the putative owner [has] established a legitimate claim to exclusivity." *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1030 (N.D. Cal. 2012) (quoting *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003)). Here, the undisputed evidence shows that, irrespective of the Pixel or EAPI, Plaintiffs' browsing data—including URL information—is shared with both their internet service providers and the advertisers whose website Plaintiffs are visiting. Ex. 29 ¶¶ 20-21; JAF-91; JAF-94. This sharing defeats exclusive control.

Plaintiffs' lack of exclusive control over this information is largely inherent to the internet's operation. "By its nature, browsing data is shared with a variety of service providers that facilitate access to the website at issue." *Lau v. Gen Digit. Inc.*, 2024 WL 1880161, at *4 (N.D. Cal. Apr. 3, 2024); *cf. Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (no reasonable expectation of privacy in information voluntarily shared with utility). Thus, as several courts in this Circuit have recently held, such data "is not capable of exclusive possession or control." *Tanner v. Acushnet Co.*, 2023 WL 8152104, at *10 (C.D. Cal. Nov. 20, 2023) (A website user's communications with a website "are not 'property' because they are not capable of

exclusive possession or control."); *Doe I*, 2024 WL 3490744, at *7 (declining to follow *Calhoun* and distinguishing the cases that it relied on).

B. PLAINTIFFS' POSITION: Plaintiffs Have a Recognized Property Interest In Their Data, Which Has Monetary Value

[redacted] *See supra* Sec. III.B.2. Yet Defendants wrongly claim that Plaintiffs lack a property interest in their collected data.

Defendants' argument rests largely on *Low v. LinkedIn Corp.*, 900 F.Supp.2d 1010, 1030 (N.D. Cal. 2012) (Koh, J.). This Court already rejected *Low* when it denied Defendants' motion to dismiss and followed Judge Koh's more recent decision in *Calhoun*, recognizing a "growing trend across courts" that "the taking of personal information was adequate to allege deprivation of a property interest." *Griffith*, 697 F.Supp.3d at 975 (citing *Calhoun*, 526 F.Supp.3d at 635). The personal information taken by Google in *Calhoun*, including "cookie identifiers," "browsing history," "IP Address," and "User-Agent," *see* 526 F.Supp.3d at 613-14 [redacted]. *Calhoun* recognized that people have a "property interest" in such information. *Id.* at 635; *accord Calhoun*, 113 F.4th at 1144 (Ninth Circuit reversing grant of summary judgment while recognizing the data categories taken by Google).

Since the Court's motion-to-dismiss order in October 2023, more courts have reached the same or similar conclusions. *See A.B. v. Google, Inc.*, 2024 WL 3052969, at *7 (N.D. Cal. Jun. 18, 2024) (personal data can be considered property under the UCL); *Kis v. Cognism, Inc.*, 2024 WL 3924553, at *7 (N.D. Cal. Aug. 23, 2024) (same); *Wall v. Wescom Central Credit Union*, 2024 WL 1158361, at *7 (C.D. Cal. Mar 18, 2024) (same); *In re Meta Pixel Tax Filing Cases*, 2024 WL 1251350, at *25 (N.D. Cal. Mar. 24, 2024) (same); *Flannery v. American Express Corp.*, 2024 WL 648689, at *4 (C.D. Cal., Jan 29, 2024) (same); *see also M.R. v. Salem Health*

Hospitals and Clinics, 2024 WL 3970796, at *8 (D. Or. Aug 28, 2024) (diminished value of personal information supports a negligence claim). The three cases cited by Defendants suggesting otherwise are against the weight of authority.

Nonetheless, Plaintiffs have also presented evidence of the "lost property value" of the data taken by TikTok. *Calhoun*, 526 F.Supp.3d at 635. Dr. Mangum calculated the objective market value of Plaintiffs' data using two comparable data collection programs, Screenwise and SavvyConnect. See Ex. 59 at ¶¶103-108. Defendants try to sweep this evidence aside because Plaintiffs "never attempted to sell" their data. That is irrelevant. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599-600 (9th Cir. 2020) (rejecting Facebook's argument that "Plaintiffs must instead demonstrate that they either planned to sell their data, or that their data was made less valuable through Facebook's use" and recognizing that "California law requires disgorgement of unjustly earned profits regardless of whether a defendant's actions caused a plaintiff to directly expend his or her own financial resources or whether a defendant's actions directly caused the plaintiff's property to become less valuable"); *CTC Real Estate Services v. Lepe*, 140 Cal.App.4th 856, 860 (Cal. App. 2006).

VII. CONCLUSION

A. Defendants' Conclusion

For these reasons, Defendants ask this Court to grant summary judgment and enter judgment for Defendants on all counts.

B. Plaintiffs' Conclusion

The Court should deny summary judgment.

Dated: October 4, 2024

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: */s/ Victor Jih*
Victor Jih

Attorney for Defendants
TikTok Inc. and ByteDance Inc.

CERTIFICATE OF COMPLIANCE

The undersigned, counsel of record for Defendants TikTok Inc. and ByteDance Inc., certifies that Defendants' sections of this joint brief contains under 7,000 words, which complies with the word limit of L.R. 11-6.1.

Dated: October 4, 2024

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: */s/ Victor Jih*
Victor Jih

Attorney for Defendants
TikTok Inc. and ByteDance Inc.

The undersigned, counsel of record for Plaintiffs, certifies that Plaintiffs' sections of this joint brief contains under 7,000 words, which complies with the word limit of L.R. 11-6.1.

Dated: September 30, 2024

BIRD, MARELLA, RHOW, LINCENBERG, DROOKS & NESSIM, LLP.

By: */s/ Ekwan E. Rhow*
Ekwan E. Rhow

Attorneys for Plaintiffs

CERTIFICATE OF COMPLIANCE

The undersigned, counsel of record for Defendants TikTok Inc. and ByteDance Inc., attests under Local Rule 5-4.3.4(a)(2) that all other signatories listed, and on whose behalf this filing is jointly submitted, concur in the filing's content and have authorized the filing.

Dated: October 4, 2024

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: */s/ Victor Jih*

Attorney for Defendants
TikTok Inc. and ByteDance Inc.